ILERNA Online

MÓDULO 06

Seguridad informática

CFGM Sistemas Microinformáticos y Redes

UF 01

Seguridad pasiva

Tema 1. Seguridad Física y Lógica

¿Qué vamos a ver?

01. UBICACIÓN FÍSICA Y CONDICIONES AMBIENTALES DE LOS EQUIPOS SERVIDORES

02. PROTECCIÓN FÍSICA DE LOS SISTEMAS INFORMÁTICOS

03. SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

04. APLICACIÓN DE LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

05. POLÍTICAS DE SEGURIDAD BASADAS EN LISTAS DE CONTROL DE ACCESO

06. POLÍTICAS DE CONTRASEÑAS; SISTEMAS BIOMÉTRICOS

07. MECANISMOS DE SEGURIDAD DE ACCESO AL SISTEMA

08. PERMISOS Y DERECHOS DE LOS USUARIOS

09. GESTIÓN DEL INVENTARIO DE LOS REGISTROS DE USUARIOS, INCIDENCIAS Y ALARMAS

Seguridad lógica: listas de control de acceso

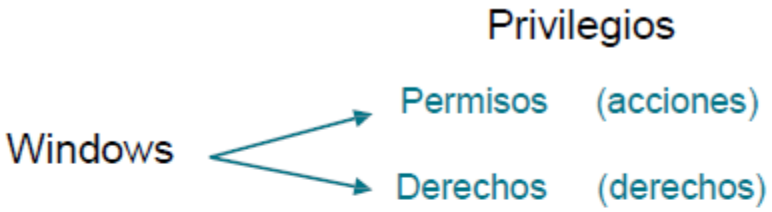
La **seguridad lógica** es la agrupación de medidas que se toman para proteger las aplicaciones y los datos y restringir el acceso solo a personas autorizadas.

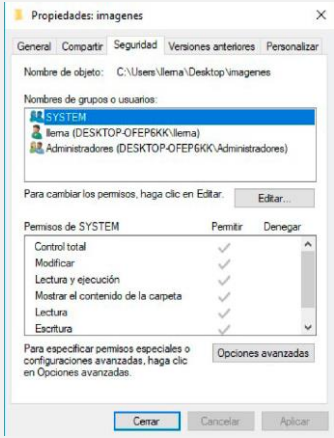
Listas de control de acceso (ACL) → Se controla que usuarios se les permite entrar y realizar determinados cambios.

- Limita el tráfico de datos
- Concede o restringe permisos y roles
- Controlas la ejecución de programas que pueden contener virus.

La encriptación

Seguridad lógica: Listas de control de acceso



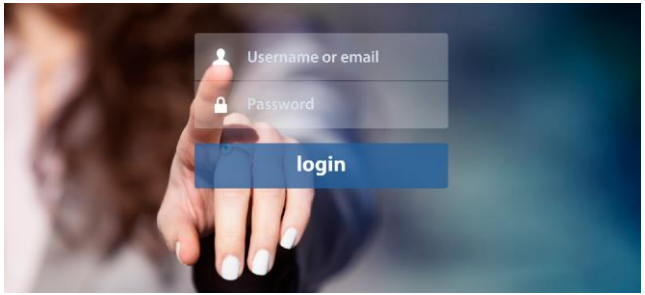



```
ubuntu20@ubuntu:/etc/tomcat9$ ls -l
total 240
drwxrwxr-x 3 root tomcat   4096 Sep 23 09:46 Catalina
-rw-r----- 1 root tomcat   7262 Feb  5  2020 catalina.properties
-rw-r----- 1 root tomcat   1400 Feb  5  2020 context.xml
-rw-r----- 1 root tomcat   1149 Feb  5  2020 jaspic-providers.xml
-rw-r----- 1 root tomcat   2799 Feb 24  2020 logging.properties
drwxr-xr-x 2 root tomcat   4096 Sep 23 09:46 policy.d
-rwxrwxrwx 1 root tomcat   7586 Sep 24 02:12 server.xml
-rwxrwxrwx 1 root tomcat   2689 Sep 24 01:47 tomcat-users.xml
-rw-r----- 1 root tomcat   2294 Sep 23 10:10 tomcat-users.xml.save
-rw-r----- 1 root tomcat   2163 Sep 23 10:10 tomcat-users.xml.save.1
-rw-r----- 1 root tomcat   2301 Sep 23 10:10 tomcat-users.xml.save.2
-rw-r----- 1 root tomcat   2294 Sep 23 10:10 tomcat-users.xml.save.3
-rw-r----- 1 root tomcat   2146 Sep 23 10:10 tomcat-users.xml.save.4
-rw-r----- 1 root tomcat   2257 Sep 23 10:40 tomcat-users.xml.save.5
-rw-r--r-- 1 root root     2316 Sep 24 00:35 tomcat-users.xmlY
-rw-r----- 1 root tomcat 172362 Feb  5  2020 web.xml
ubuntu20@ubuntu:/etc/tomcat9$ chmod 777 tomcat/users.xml
```

Seguridad lógica: políticas de contraseña

La autentificación de los usuarios de realiza introduciendo un nombre y una **contraseña**

Las contraseñas deben seguir una serie de recomendaciones



Seguridad lógica: sistemas biométricos

Los sistemas biométricos se utilizan para autentificar a los usuarios a través de sus rasgos físicos y conductas (características inalterable)

Dos módulos

- Inscripción
- identificación

Dos sectores

- Verificación anatómica
- Verificación de la identidad por el comportamiento

Es muy costoso

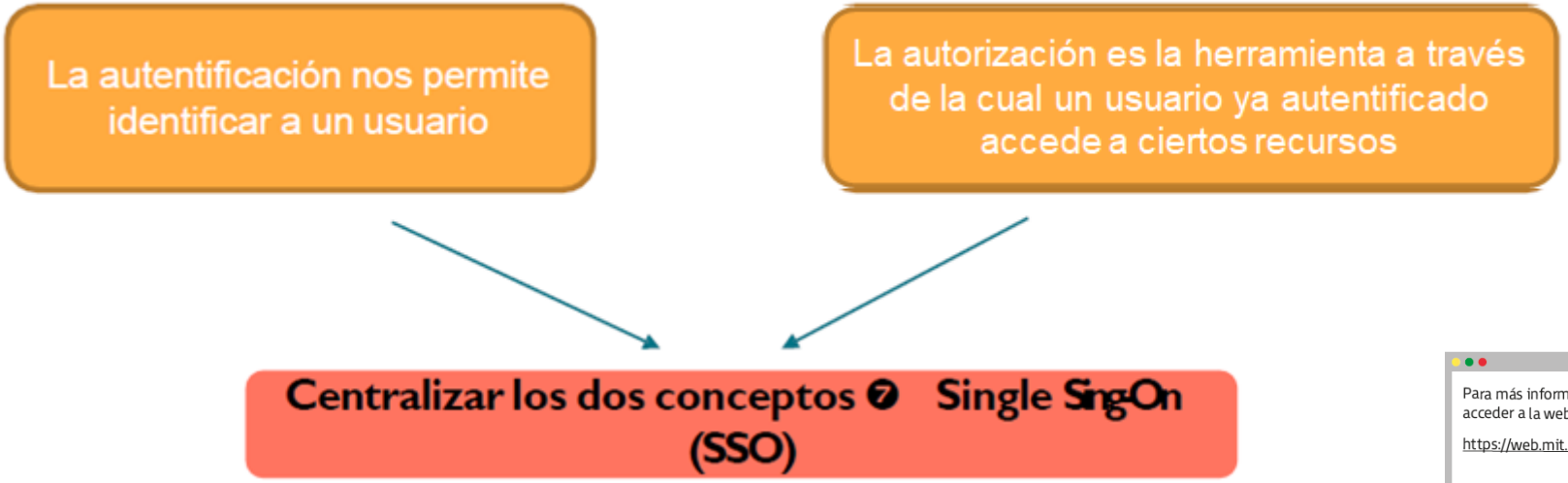
Seguridad lógica: mecanismos de seguridad de acceso al sistema

Mecanismos físicos

- Dispositivo de teclado
- Dispositivos por tarjetas

Se consideran accesos a todas aquellas aberturas o espacios de comunicación con el exterior, no solo puertas y ventanas, sino también conductos de refrigeración, garajes…

Seguridad lógica: métodos para la autenticación



BUSCA EN LA WEB

Para más información podemos acceder a la web de **Kerberos**:

https://web.mit.edu/kerberos/

¿DUDAS?

MÓDULO 06

Seguridad informática

CFGM Sistemas Microinformáticos y Redes

Conceptos Interesantes

Seguridad Informática

- Conjunto de métodos y herramientas destinados a proteger la información (y a los sistemas informáticos que la contienen) ante cualquier amenaza.
- Es un proceso en el cual participan además personas; y concienciarlas de su importancia en el proceso será de gran importancia.

Conceptos Interesantes

¿Qué es la Criptografía?

- Es una rama que su raíz está en las matemáticas;
- Hace uso de uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Según la RAE:

"Arte de escribir con clave secreta o de modo enigmático"

Conceptos Interesantes

¿Qué es la Cifra o cifrado o encriptado?

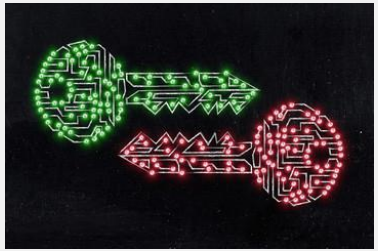
- Técnica que protege/autentica a un documento/usuario al aplicar un algoritmo criptográfico.
- Sin conocer una clave específica o secreta, no será posible descifrarlo o recuperarlo.

Timetoast Sistemas de cifrado

Conceptos Interesantes

Otras Definiciones importantes

- **Criptología**: ciencia que estudia e investiga todo aquello relacionado con la criptografía: incluye cifra y criptoanálisis.
- **Criptógrafo**:
  - Persona que cifra o descifra mensajes escritos con clave secreta
  - Máquina o artilugio para cifrar.
- **Criptoanalista**: persona cuya función es romper algoritmos de cifra en busca de debilidades, la clave o del texto en claro.



- **Texto en claro**: documento original. Se denotará como M.
- **Criptograma**: documento/texto cifrado. Se denotará como C.
- **Claves**: datos (llaves) privados/públicos que permiten cifrar un documento y descifrar el correspondiente criptograma.

Preguntas interesantes

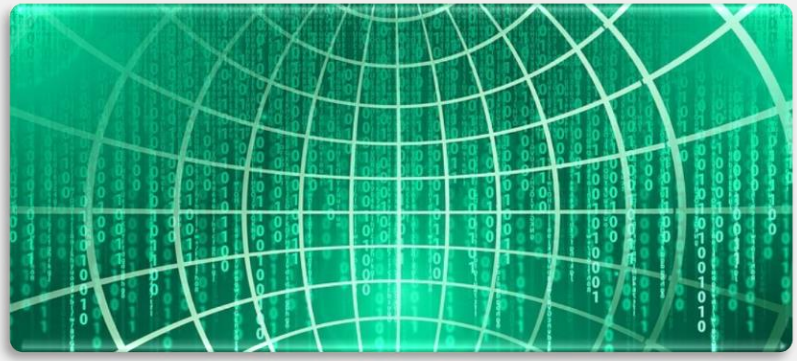
¿Cuáles son los puntos débiles de un sistema informático?

- Un usuario no deseado para acceder al sistema; utilizará el artilugio que le haga más fácil su acceso y posterior ataque
- Existirá una diversidad de frentes desde los que puede producirse un ataque, tanto internos como externos.

Preguntas interesantes

¿Cuánto tiempo deberá protegerse un dato?

- Los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor como tal.
- Estamos hablando, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
- Esto nos llevará a la fortaleza del sistema de cifra.



Preguntas interesantes

¿Medidas de control?

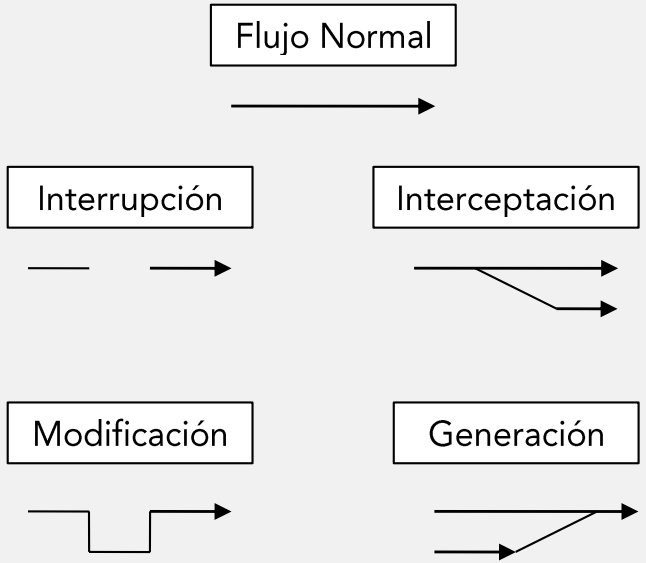
- Las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.
    - Efectivo: que funcionen en el momento oportuno.
    - Eficiente: que optimicen los recursos del sistema.
    - Apropiadas: que pasen desapercibidas para el usuario.

Ningún sistema de control resulta efectivo hasta que debemos utilizarlo al surgir la necesidad de aplicarlo.

Conceptos Interesantes

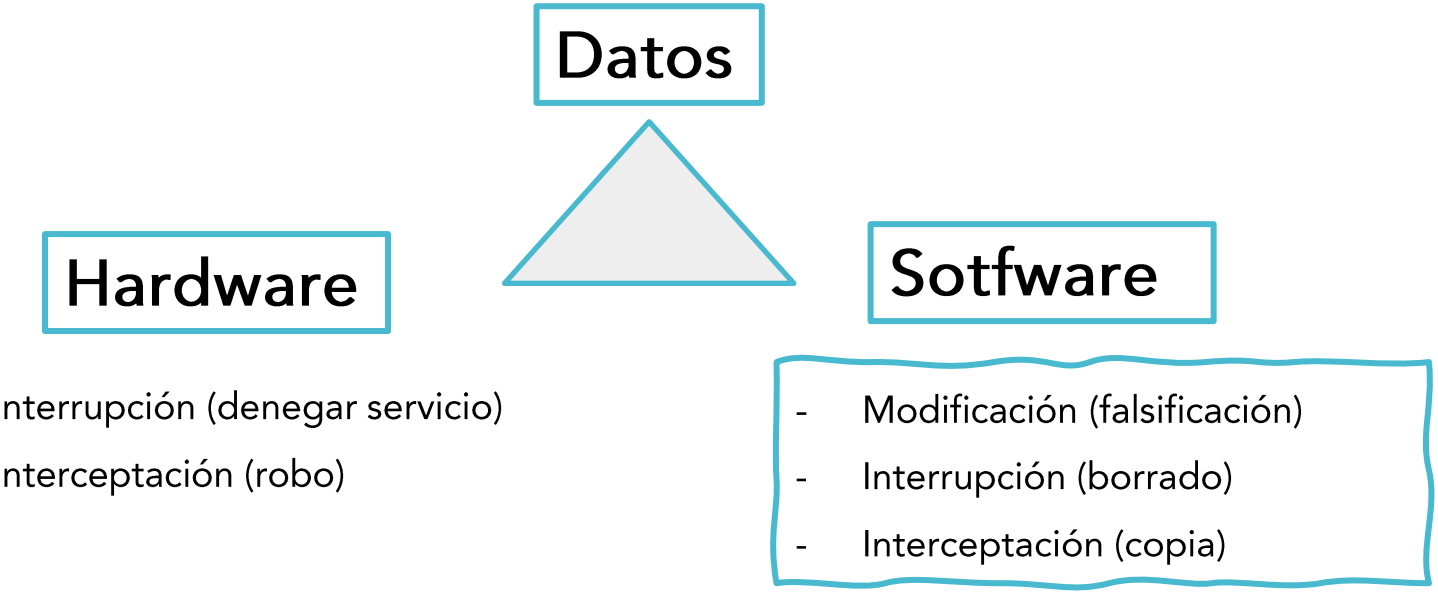
Amenazas del sistema

- Las amenazas afectan principalmente al hardware, al software y a los datos.
- Son causadas por:
  - Interrupción
  - Interceptación
  - Modificación
  - Generación



Escenarios amenazas del sistema

Interrupción (pérdida)	Interceptación (acceso)	Modificación (cambio)	Generación (alteración)



Conceptos Interesantes

Debilidades del sistema

- **Hardware:** pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- **Software:** puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- **Datos:** puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

- **Memoria:** puede producirse la introducción de un virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- **Usuarios:** puede producirse la suplantación de identidad, el acceso no autorizado, visualización de datos confidenciales, etc.

¿DUDAS?

MÓDULO 06

Seguridad informática

CFGM Sistemas Microinformáticos y Redes